



February 7, 2014

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW, Suite TW-A325
Washington, D.C. 20554

**RE: EB Docket No. 06-36
Section 64.2009(e) CPNI Certification
CenCom, Inc. (Form 499-A Filer ID No. 821484)**

Dear Ms. Dortch:

Pursuant to the Commission's Public Notice, DA 14-138, released on February 5, 2014, attached for filing is a section 64.2009(e) Customer Proprietary Network Information certification and accompanying statement covering the prior calendar year of 2013 of CenCom, Inc. (Form 499-A Filer ID No. 821484).

Respectfully submitted,

David Armstrong
President

A handwritten signature in blue ink, appearing to read "David M. Armstrong", is written over the printed name and title.

Attachment

cc: Best Copy and Printing, Inc.
Portals II
445 12th Street, Suite CY-B402
Washington, D.C. 20554
fcc@bcpiweb.com



Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

1. Date filed: 2/7/14
2. Name of company covered by this certification: CenCom, Inc.
3. Form 499 Filer ID: 821484
4. Name of signatory: David Armstrong
5. Title of signatory: President
6. Certification:

I, David Armstrong, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.
See 47 C.F.R. § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

A handwritten signature in blue ink, appearing to read "David Armstrong", is written over a horizontal line. Below the line, the name "David Armstrong" is printed in a small, black, sans-serif font.

[David Armstrong]

Attachment: Accompanying Statement explaining CPNI procedures

CenCom, Inc.: CPNI Operating Procedures

OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

CenCom, Inc. (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training:

The Compliance Officer arranges for the training of all personnel on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when personnel are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all personnel are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. Each employee has his own CPNI manual.

Personnel are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all personnel.

A copy of the Company's disciplinary process is kept in the CPNI manual.

Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers of their CPNI rights and has asked for the customer's approval to use CPNI via the opt-out method. A copy of the notification is also provided to all new customers that sign up for service.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed so that personnel can readily identify customers that have restricted the use of their CPNI.

For the customers that have opted-out and said the Company cannot use their CPNI, that decision will remain valid until the customer changes it.

The company sends the opt-out notice every two years to those customers that have not previously opted out.

CenCom, Inc.: CPNI Operating Procedures

Notification of Breaches

Personnel will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.
- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.
- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

Record Retention

The Company retains all information regarding CPNI in a CPNI file in the office vault. Following is the minimum retention period we have established for specific items:

- CPNI notification and records of approval – one year
- Marketing campaigns – one year
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years

Miscellaneous

The Company's CPNI policies include reasonable measures to discover and protect against activity that is indicative of pretexting. Employees are instructed to notify the CPNI Compliance Officer if any such activity is suspected.